NIAC
NEBRASKA INFORMATION ANALYSIS CENTER

Privacy Policy

Approved by NIAC Executive Board January 2024

A. Purpose Statement

The mission of the Nebraska Information Analysis Center (NIAC) is to collect, evaluate, analyze, and disseminate Suspicious Activity Reports (SARs) and intelligence regarding criminal and terrorist activity to federal, state, local, and tribal law enforcement agencies, other Fusion Centers, and to private entities, as appropriate, in the interests of critical infrastructure protection, counterterrorism, law enforcement situational awareness and public safety. This public safety mission includes analytic support in the event of hazards, such as severe weather, disease, floods, and other emergencies, as appropriate.

The NIAC's Privacy Policy is designed for fusion center personnel and authorized users to ensure that they are aware of, and comply with, the legal and privacy framework in which the NIAC operates, as well as to support the publics and other agencies' confidence in the NIAC's ethical and lawful responsibility to protect privacy, civil rights, and civil liberties.

B. Policy Applicability and Legal Compliance

All Nebraska State Patrol (NSP) and NIAC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with this policy. The NIAC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties, including but not limited to, the Constitution of the United States of America; applicable civil rights acts; 28 CFR Parts 20, 22, and 23; the Electronic Communications Privacy Act of 1986; the Constitution of the State of Nebraska; and applicable Nebraska statutes.

The NIAC will provide access to a printed, electronic, or online copy of this policy to all center and non-center personnel who provide services, and to participating agencies and individual users.

The NIAC's Privacy Policy will be provided to the public upon request. It is posted on the center's publicly available website located at: https://statepatrol.nebraska.gov/divisions/investigative-services/nebraska-information-analysis-center

C. Governance and Oversight

The NIAC Executive Board was established to provide guidance and oversight regarding NIAC operations, as well as short, and long-term objectives. The Executive Board meets approximately every quarter of the calendar year. Primary responsibility for the operation of the NIAC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, and evaluation of information; information quality, analysis, destruction, sharing, or disclosure; and the enforcement of this policy, is tasked to the NIAC Director.

The Executive Board directed the NIAC to develop a Privacy Policy. The Executive Board ensures that privacy and civil rights are protected within the provisions of this policy and within the NIAC's information collection, retention, and dissemination processes and procedures. The Executive Board has mandated that the policy be reviewed and updated, as appropriate.

The NIAC's Privacy Officer is the Nebraska State Patrol Assistant General Counsel, or designee. The Privacy Officer: receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and ensures that enforcement procedures and sanctions outlined in Section N.3 are adequate and enforced. The NIAC Privacy Officer serves as the liaison for the Information Sharing Environment, as needed, and ensures that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following address: Nebraska Information Analysis Center, Attn: Privacy Officer, 4600 Innovation Drive, Lincoln, NE 68521.

D. Definitions

Primary terms and definitions used in the NIAC Privacy Policy are in Appendix A.

E. Information

The NIAC's Watch Center serves as the focal point for the receipt and dissemination of criminal and terrorism intelligence, Suspicious Activity Reports (SARs) as well as requests for services (RFS) from participating agencies. NIAC's information is received from, and disseminated to, local, state, federal, and tribal law enforcement; other Fusion Centers; the public; and to private entities, as appropriate. All requests for information are noted in the state intelligence database.

The NIAC will seek, view and/or retain information that:

- Is based on a criminal predicate or threat to public safety
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense, or is involved in, and/or planning, criminal or terrorist conduct or activity that presents a threat to any individual, community, or the nation, and that the information is relevant to the criminal or terrorist conduct

- Is relevant to the investigation and prosecution of suspected criminal or terrorist incidents; the resulting justice system response; the enforcement of sanctions, orders, and sentences; or the prevention of crime
- Is useful in crime analysis, or in the administration of criminal justice and public safety (including topical searches)

The NIAC may retain information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads, and information that is reasonably indicative of pre-operational planning related to terrorism or other criminal activity, such as Suspicious Activity Reports (SAR) or Information Sharing Environment (ISE) SAR (ISE-SAR) information. The ISE is a conceptual framework composed of the policies, procedures and technologies linking the resources of State, Local, Tribal and Territorial agencies, federal agencies, and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

The NIAC will not seek or retain information about individuals or organizations solely based on their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

The NIAC applies labels to information, as appropriate, to indicate to the accessing authorized user that:

- The information is protected information, as defined by the center, to include personal data on any individual (see definitions of "protected information" and "personally identifiable information" in Appendix A)

- The information is subject to local, state, or federal law restricting access, use, or disclosure.

Upon the receipt of information, NIAC personnel will evaluate the information to determine its nature, usability, and quality. NIAC personnel will assess information to ensure proper segregation, such as:

- Whether the information is based upon a standard of reasonable suspicion of criminal activity
- Whether the information consists of tips and leads, data, or Suspicious Activity Reports
- The nature of the source of the information as it affects its veracity (for example, whether from an anonymous tip, trained interviewer or investigator, public record or from the private sector)
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown)

- The validity of the content (for example, verified, partially verified, unverified, or unable to verify)
- What level of protection is to be afforded the information based upon the type of information received, and to what extent it may be shared through the Information Sharing Environment (ISE)

At the time a decision is made by the NIAC to retain information, it will be labeled to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Protect confidential sources and law enforcement undercover techniques and methods
- Not interfere with or compromise pending criminal investigations
- Protect an individual's right of privacy or his or her civil rights and civil liberties
- Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter

The labels assigned to existing information will be re-evaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

NIAC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and Suspicious Activity Report (SAR) information. Center personnel will:

- Prior to allowing access to, or dissemination of, the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value, and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful.
- Store the information using the same storage method used for criminal intelligence, which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.

- Allow access to, or disseminate, the information using the same (or a more restrictive) access or dissemination standard that is used for criminal intelligence (for example, "need-to-know" and "right-to-know" access).
- Regularly provide access to, or disseminate, the information to appropriate intelligence consumers in response to an interagency inquiry for law enforcement, homeland security, or public safety and crime analytic purposes
- Follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in the state intelligence database.

NIAC personnel, partners and participating agencies will be required to adhere to specific practices and procedures for the receipt, collection, assessment, marking, storage, access, dissemination, retention, and security of tips and leads, and SARs information.

The NIAC will incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information as well as constitutional rights, including personal privacy and other civil liberties.

The NIAC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

- The name of the originating center, department or agency, component, and subcomponent
- The name of the center's justice information system from which the information is disseminated
- The date the information was collected and, where feasible, the date its accuracy was last verified
- The title and contact information for the person to whom questions regarding the information should be directed

In the interests of information/intelligence security, all NIAC products which include Personally Identifiable Information (PII), operationally sensitive details, investigative information, and/or similarly law enforcement sensitive information shall be marked Law Enforcement Sensitive (LES). Only law enforcement officers and/or intelligence personnel with a need-to-know and right-to-know are provided with such a NIAC product. Additional reasons for a Law Enforcement Sensitive marking include:

- Protecting confidential sources and law enforcement investigative methods
- Ongoing criminal investigative information
- Protect the due process rights of a possible suspect

F. Acquiring and Receiving Information

The NIAC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

Additionally, the NIAC provides for the following analytic vetting process upon receiving a Suspicious Activity Report:

- Initial review to ensure that the information was legally obtained
- Attempt to detect behaviors and incidents indicative of terrorist activity
- Review the SAR against all available knowledge and information for linkages to other suspicious or criminal activity
- Determine if the SAR is solely based on an impermissible characteristic, such as race, ethnicity, religion, or 1st Amendment protected activity; in such a case, the SAR is not retained nor forwarded.

Based on this review, the analyst will apply his or her professional judgment to determine whether the information has a potential nexus to terrorism.

- If the analyst cannot make this explicit determination, the report will not be accessible by the ISE, although it may be retained in the NIAC's files, in accordance with its established retention policies and business rules
- If the analyst can determine that a SAR has a direct connection to possible terrorism- related criminal activity, the information will be considered an ISE-SAR, and the analyst will provide the information to the local JTTF and E-Guardian for use as the basis for an assessment or investigation

When the NIAC enters a contract with a business or corporate entity, they will provide the NIAC with an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations, and that these methods are not based on misleading information collection practices.

The NIAC will not directly or indirectly receive, seek, accept, or retain information from an individual who, or information provider that is, legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

The NIAC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; is accurate, current, and complete, including the relevant context in which it was sought or received; and that the information about the same individual or organization is merged only after utilizing the applicable standards. The NIAC will record the sources of all information that is retained.

The NIAC reviews, in a timely manner, alleged errors and deficiencies, and corrects, deletes, or refrains from using protected information found to be erroneous or deficient. The labeling of retained information will be re-evaluated when new information is received that has an impact on the confidence (validity and reliability) of the previously retained information.

The NIAC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer, in such a case, the NIAC would consult the NSP Legal Division prior to the use of the information.

Originating agencies external to the NIAC are responsible for the quality and accuracy of the data accessed by, or provided to, the NIAC. The NIAC will advise, in writing, the appropriate contact person of the originating agency if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

The NIAC will use a written or documented electronic means of notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the NIAC; for example, when the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the individual may be affected.

H. Collation and Analysis

Information acquired or received by the NIAC, or accessed from other sources, will be analyzed only by qualified individuals who have successfully completed a background check and retain appropriate security clearance, if applicable, and who have been selected, approved, and trained accordingly.

Information acquired or received by the NIAC, or accessed from other sources, is analyzed according to priorities, and needs only to:

- Further crime or terrorism prevention, law enforcement, force deployment, or prosecution objectives and priorities established by the NIAC, and

- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in, or engaging in, criminal or terrorist activities.

I. Merging Records

Criminal intelligence about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of a match.

The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject, and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, marks or scars; social security number; driver's license number; or other biometrics such as DNA, or facial recognition. Identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization or subject.

If the matching requirements are not fully met, but there is an identified partial match, the information may be associated if accompanied by a clear analytic statement that it has not been adequately established that the information relates to the same individual or organization.

J. Sharing and Disclosure

The NIAC Director, or designee, shall establish requirements and records for all personnel as to their access authority and permission to access NIAC's information. Permissions regarding viewing, adding, editing, and printing of NIAC information will be controlled by NIAC's administrator(s). All NIAC personnel, with approval from the NIAC Director may disclose NIAC information pursuant to applicable policy;

Access to, or disclosure of, records retained by the NIAC will be provided only to persons within the NIAC or in other governmental agencies who are authorized to have access, and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes, and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of everyone who accessed information retained by the center and the nature of the information accessed, will be kept by the center.

Information gathered and records retained by the NIAC will not be:

- Sold, published, exchanged, or disclosed for commercial purposes

- Disclosed or published without prior notice to the originating agency that such information is subject to re-disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency
- Disseminated to persons not authorized to access or use the information.

There are several categories of records that will ordinarily not be provided to the public:

- Protected federal, state, local, or tribal records, which may include records originating with and controlled by, another agency that cannot be shared without permission; see also 6 U.S.C. sec 482(e) which preempts state and local disclosure of federal "Homeland Security Information" requested pursuant to an open records request submitted under state law
- 84-712.05 which enumerates all records which may be withheld from the public
- 28-722 which states that the Department of Health and Human Services shall not release data that would be harmful, detrimental, or would reveal the identity of a reporter of child abuse or neglect
- 29-4009 lists certain information that the Sex Offender registry shall not release, such as personal information or victim's name
- 60-484.02 is the DMV section on digital signatures and images. They cannot be disclosed to anyone outside of law enforcement
- 60-2905 Prohibits disclosure of personal information obtained from DMV without written consent of the person to whom the information pertains
- A violation of the above statutes could result in civil or criminal penalties as defined in each of the statutes listed above.

The NIAC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information, unless otherwise required by law.

K. Redress

K.1 Disclosure

Requests for disclosure of NIAC records by the public will be referred to the NSP Legal Division for response. A record will be kept of all requests and of what information is disclosed to an individual.

The existence, content, and source of the information will not be made available to an individual when:

- Disclosure to the individual is exempt or prohibited by applicable U.S. Code, Nebraska State Statute, or administrative rule.

K. 2 Complaints and Corrections

If an individual has complaints or objections to the accuracy or completeness of information about him or her originating from NIAC information, the NIAC will inform the individual of the procedure for submitting complaints or objections (if not properly communicated), or to request corrections. If an individual's complaint or objection cannot be resolved after review at the NIAC, the individual may request a review of that decision by the NIAC Executive Board. A record will be kept of all complaints and requests for corrections as well as the resulting actions, if any.

If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates with another agency, the NIAC will notify the source agency of the complaint or request for correction in writing or electronically within 10 days and, upon request will coordinate with the source agency to assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate, and to ensure that the individual is provided with applicable complaint submission or corrections procedures. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. A record will be kept by the center of all such complaints and requests for corrections as well as resulting actions, if any.

The individual who has requested disclosure, or to whom information has been disclosed, will be given reasons if disclosure or requests for corrections are denied by the NIAC or the originating agency. The individual will also be informed of the procedure for appeal when the center or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

K.3 Redress

If an individual has complaints or objections to the accuracy or completeness of NIAC/ISE-SAR information allegedly held by NIAC, and that has resulted in specific, demonstrable harm to such individual, NIAC will inform the individual of the procedure for submitting complaints or requesting corrections (if not properly communicated). Complaints will be received by the center's Privacy Officer at the following address: Nebraska Information Analysis Center, Attn: Privacy Officer, 4600 Innovation Drive, Lincoln, NE 68521. The Privacy Officer will acknowledge the receipt of the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of any NIAC/ISE-SAR information in privacy fields that identifies the individual unless otherwise required by law. Any personal information will be reviewed and corrected in or deleted from NIAC/ISE-SAR shared space if the information is determined to be erroneous, includes incorrectly merged information, or is out of date. A record will be kept of all complaints and requests for corrections as well as the resulting actions, if any.

The NIAC will further delineate protected information shared through the ISE from other data the NIAC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

L. Security Safeguards

A NIAC Research Manager is designated and trained to serve as the center's security liaison. The NIAC is in a secure facility within the Headquarters Troop area of the NSP, protected from external intrusion. The NIAC's office space is only accessible to NIAC personnel, partners, and participating agencies, and other authorized NSP personnel. The NIAC will utilize secure internal and external safeguards against network intrusions. Access to NIAC's system from outside the facility will be allowed only over secure networks.

The NIAC will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged, except by personnel authorized to take such actions.

The NIAC will notify an individual whose personal information was, or is, reasonably believed to have been breached or obtained by an unauthorized person, and for whom such unauthorized access may result in physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of unauthorized access to the information, and consistent with the legitimate needs of law enforcement to investigate the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

M. Information Retention and Destruction

All NIAC-generated applicable intelligence and/or information furnished to the NIAC, some of which may be for dissemination, will be reviewed for record retention (validation or purge) at least every five years, as provided by 28 CFR Part 23.

When information has no further value or meets the criteria for removal according to the NIAC's retention and destruction policy, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency. A record of information to be reviewed for retention will be maintained by the NIAC.

The NIAC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

No approval will be required from the originating agency before information held by the NIAC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

Notification of proposed destruction or return of records may or may not be provided to the originating agency by the NIAC, depending on the relevance of the information and any agreement with the originating agency.

N. Accountability and Enforcement

N. 1 Information System Transparency

The NIAC's Privacy Officer will be responsible for receiving inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s). The privacy officer can be contacted at the following address: Nebraska Information Analysis Center, Attention: Privacy Officer, 4600 Innovation Drive, Lincoln, NE 68521. The NIAC Privacy Officer will report all inquiries and complaints to the NSP's Legal Department. The Legal Department will direct the handling and response to inquiries and complaints.

N. 2 Accountability

A record will be kept for a minimum of five years for access to information for specific purposes and of what information is disseminated to each person in response to the request.

The NIAC's Privacy Officer will periodically conduct audits to ensure and evaluate the compliance of users. The Privacy Officer will conduct an annual audit and inspection of the Watch Center's information. Random audits of information and compliance will be performed as deemed appropriate by the Privacy Officer.

The NIAC's personnel, or other personnel participating with the NIAC, shall report violations or suspected violations of NIAC policies relating to protected information to the NIAC's Privacy Officer and/or the NIAC Executive Board.

The NIAC's Executive Board, guided by the trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy at least annually and will make appropriate changes in response to changes in applicable law, technology, purpose and use of the information systems, and public expectations.

N.3 Enforcement

If an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification or disclosure of information, the Privacy Officer will:

- Notify, in writing, the chief executive of the employing agency of the noncompliance of his or her employee of the violation.
- Initiate an investigation, criminal, if appropriate.

In addition:

- As the NIAC is a multi-agency effort, the NIAC Director will work with each agency regarding their personnel policies for appropriate sanctions that do not rise to a criminal matter
- Agencies must take action to correct such violations and provide an assurance in writing, to the Director of the NIAC that corrective action has been taken
- The failure to remedy violations may result in suspension or termination of access for the employee to NIAC information
- The NIAC reserves the right to restrict the access level and the number of personnel having direct access to NIAC information, and to suspend or withhold service to any participating agency user who fails to comply with the applicable restrictions and limitations of the NIAC's privacy policy

O. Training

The NIAC will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

The NIAC will require annual training for the following individuals regarding implementation of and adherence to the privacy policy:

- Any person that is granted direct access to NIAC information
- Personnel authorized to share protected information through the Information Sharing Environment.

The NIAC's privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the NIAC
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user
- The impact of improper activities associated with infractions within, or through, the agency
- Mechanisms for reporting violations of NIAC privacy-protection policies
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any
- Originating and participating agency responsibilities and obligations under applicable law and policy.

Appendix A - Definitions

Access—Data access refers to the ability to get to data on a computer. Web access refers to having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only or read/write access.

With regard to the Information Sharing Environment, access refers to the business rules, means, and processes by, and through which, Information Sharing Environment participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another Information Sharing Environment participant.

Access Control—Mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role based.

Agency—Agency refers to the NIAC and all agencies that access, contribute, and share information in the NIAC's justice information system.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log- ins and logouts. More expansive audit trail mechanisms would record each user's activity in detail; what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security and are used to trace unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provides adequate credentials that prove identity. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of usernames and passwords.

Authorization—The process of granting a person, computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access, and that is verified through authentication. *See Authentication*.

Authorized User—A person that is granted direct access to NIAC information.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. Implementations of the latter include voiceprints and handwritten signatures.

Civil Rights—The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual; therefore, civil rights are obligations imposed on government to promote equality. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against based on any federally or state protected characteristic.

Civil Liberties—Civil liberties are fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Computer Security—The protection of information assets using technology, processes, and training.

Credentials—Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of, and the criminal activity engaged in, by an individual or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures.

Data Protection—Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes, but which is not available to everyone.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, for example electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems.

General Information or Data—Information that may include records, documents, or files pertaining to law enforcement operations such as computer-aided dispatch (CAD) data, incident data, and management information; and information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Information—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Identification—A process whereby a real-world entity is recognized, and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code specifically designed as an identifier, or a collection of data such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

Information Quality—Information quality refers to various aspects of the information such as the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Invasion of Privacy—Invasion of privacy can be defined as intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. *See also Right to Privacy*.

Law—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information—For purposes of the Information Sharing Environment, law enforcement information means any information obtained by, or of interest to, a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland; and (b) relevant to a law enforcement mission, including, but not limited to, information pertaining to an actual or potential criminal, civil, or administrative investigation, or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of, or response to, criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved, or suspected of involvement, in criminal or unlawful conduct; or assisting, or associated with, criminal or unlawful conduct; the existence, identification, detection, prevention,

interdiction, or disruption of, or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Logs—Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals have access to the data. *See also Audit Trail*.

Maintenance of Information—The maintenance of information applies to all forms of information storage. This includes electronic systems (for example, databases) and non- electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information, or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information; more specifically, information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know – As a result of jurisdictional, organization, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Data—Personal data refers to any information that relates to an identifiable individual. *See also Personally Identifiable Information*.

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, marks, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AFIS] identifier, or booking or detention system number).

- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information associated with an individual(s).

Privacy—Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of
information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—Protected information is information about any individual that is subject to information privacy or other legal protections under the Constitution and laws of the United States and the State of Nebraska.

Record—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by, or for, the collecting agency or organization.

Redress—Internal procedures to address complaints from persons regarding protected information about them that is under the agency's/center's control.

Retention—*Refer to Storage*.

Right to Know – Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counter-terrorism activity.

Right to Privacy—The right to be left alone in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Authorization—A type of authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—Security refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set as well as promoting failure resistance in the electronic systems overall.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. With regard to the Information Sharing Environment, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland, by both the originator of the information and any recipient of the information.

Suspicious Activity—Suspicious activity is defined as "reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention." Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber-attacks, testing of security, etc.

Suspicious Activity Reports—The observation and documentation of a suspicious activity. Suspicious activity reports offer a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR data analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center.

Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to:
(a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism, (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (c) communications of or by such groups or individuals, or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information—In accordance with IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the Information Sharing Environment facilitates the sharing of terrorism information, including weapons of mass destruction information, and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the Information Sharing Environment will

facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Tips and Leads Information or Data—Uncorroborated reports or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data. Tips and leads information is maintained in a secure system similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.